UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION

MICHAEL CLIVER and MARY CLIVER, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

vs.

INDEPENDENT LIVING SYSTEMS, LLC,

Defendant.

Civil Action No.: 1:23-cv-21134

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Michael Cliver ("Michael Cliver" or "Mr. Cliver") and Mary Cliver ("Mary Cliver" or "Mrs. Cliver") (collectively, "Plaintiffs"), individually and on behalf of all other persons similarly situated, by and through their attorneys, upon personal knowledge as to their own acts and experiences, and upon information and belief as to all other matters, allege as follows:

NATURE OF THE ACTION

1. Plaintiffs Michael Cliver and Mary Cliver bring this Class Action Complaint against Defendant Independent Living Systems ("ILS" or "Defendant") to seek recovery on behalf of themselves and over 4 million similarly situated people ("Class Members"), based upon Defendant's failure to properly secure and safeguard the sensitive personally identifiable information ("PII") and protected health information ("PHI") (collectively, "PII") of individuals receiving healthcare administrative services from ILS and/or its affiliates.

2. Specifically, Defendant failed to properly protect Plaintiffs' and Class Members' names, addresses, dates of birth, drivers' licenses, state identification, Social Security numbers, financial account numbers, Medicare or Medicaid identification, CIN#, mental or physical treatment/condition information, diagnosis code or diagnosis information, admission/discharge dates, prescription information, billing/claims information, and health insurance information, which was collected by ILS by virtue of its business associations with health insurers HPMP of Florida, Inc. d/b/a Florida Complete Care, and Florida Community Care, LLC. This information is considered PII because it can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR §200.79.

3. An unauthorized actor gained access to ILS's computer systems between June 30 and July 5, 2022. During that period, PII that was stored on Defendant's computer systems was accessed and viewed by the unauthorized actor. Defendant later determined that the PII accessed and viewed included Plaintiffs' and Class Members' PII (the "Data Breach"). The Data Breach was so serious that it rendered portions of ILS's computer systems inoperable. The Company did not receive the results of the review of the circumstances underlying the Data Breach until almost six (6) months later in January of 2023. Thereafter, ILS "validated" the results and issued notice to impacted individuals in March of 2023. This was a follow-up to the earlier preliminary notice posted by the Company on its website.

4. As required by state laws across the country, Defendant sent templates of the Notice of Data Breach Letter to state attorneys general. Specifically, Defendant sent a template of the Notice of Data Breach Letter to the Maine Attorney General and identified that approximately 4,226,508 individuals like Plaintiffs had their PII accessed, exfiltrated, and/or compromised on the

Data Breach.[1]

5. The Data Breach occurred because Defendant did not implement adequate and reasonable cyber-security procedures and protocols to protect Plaintiffs' and Class Members' PII. Because Defendant's data security protocols and practices were deficient, unauthorized person(s) were able to access, view, and/or exfiltrate Plaintiffs' and Class Members' PII. Notably, in its March 14, 2023 Supplemental Notice of Data Event, the Company acknowledged that "it promptly took steps to mitigate any risk of compromise to information and to better prevent a similar event from reoccurring."[2] The fact that Defendant enhanced its security features post-Data Breach indicates Defendant's cybersecurity measures were inadequate, negligent, and lacking at the time of the Data Breach.

6. Defendant failed to properly safeguard Plaintiffs' and Class Members' PII. Defendant's negligence has caused millions of Class Members harm and puts them at a substantially increased risk of identity fraud, which will negatively impact them for years.

7. Defendant is wholly responsible for this Data Breach through its failure to implement and maintain adequate and reasonable data security safeguards, and failure to comply with industry-standard data security practices and federal and state laws and regulations governing data security and privacy, including security of PII.

8. Defendant failed to timely recognize and detect unauthorized access and use of its systems and failed to timely recognize the substantial amounts of data that had been compromised.

9. Defendant failed to, among other things: (1) timely detect any unauthorized actors had accessed its file servers; (2) notice the massive amounts of data that were compromised and

---

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec.shtml (last visited Mar. 19, 2023).

[2] https://ilshealth.com/supplemental-data-notice (last visited Mar. 19, 2023).

accessed; and (3) take any steps to investigate the red flags that should have warned Defendant that its systems were not secure.

10. Moreover, if Defendant properly maintained and monitored its information technology infrastructure and denied access to that infrastructure to all potential threats, Defendant would have either prevented the Data Breach altogether or at the very least discovered the invasion sooner.

11. Defendant had numerous statutory, regulatory, and common law duties to Plaintiffs and Class Members to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

12. Defendant was and remains required to maintain the security and privacy of the PII entrusted to it. When Plaintiffs and Class Members provided their PII, Defendant and its agents were required to comply with the obligation to keep Plaintiffs' PII secure and safe from unauthorized access, to use this information for business purposes only, and to make only authorized disclosures of this information.[3]

13. Defendant was cognizant of the ever-growing and ever-present threat of cybersecurity attacks. Despite this awareness, Defendant failed to properly safeguard Plaintiffs' and Class Members' information. This makes Defendant's failure particularly egregious.

14. By virtue of Defendant's business practices, Defendant represented to Plaintiffs and Class Members that it would protect their PII.

15. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII by entrusting their PII to a company that represented it would protect and safeguard their PII.

---

[3] https://ilshealth.com/privacy-policy/ (last visited Mar. 19, 2023).

16. Plaintiffs' and Class Members' PII was accessed and downloaded by one or more unauthorized actors because Defendant failed to properly protect the PII of Plaintiffs and Class Members.

17. Because of Defendant's failure to properly protect the PII in its possession, Plaintiffs and Class Members are now at a significant present and future risk of identity theft, healthcare fraud, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

18. Defendant's conscious decision to delay notifying Plaintiffs and Class Members for many months exacerbated the harm that Plaintiffs and Class Members have and will experience. Moreover, Plaintiffs and Class Members were unable to take actions to protect themselves and attempt to mitigate the harm until they received notice.

19. Plaintiffs and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft;

c. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach;

d. The emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach;

e. The actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals and made available on the Dark Web;

f. Damages to and diminution in value of their personal data;

g. Actual damages in the form of the difference in value between the services that should have been delivered and the services that were in fact delivered; and

h. The continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

20. Plaintiffs seek to remedy these harms and future harms on behalf of himself and all similarly situated persons.

21. Accordingly, Plaintiffs, on behalf of themselves and Class Members, assert claims for negligence. Plaintiffs and Class Members seek injunctive relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiffs

22. Plaintiff Michael Cliver is a citizen of Orange County, Florida. Mr. Cliver, a Medicare subscriber, received healthcare services through Florida Complete Care in June of 2022. Florida Complete Care utilized the administrative services of ILS. He received notice that his PII was improperly exposed to unauthorized third parties by ILS.

23. Plaintiff Mary Cliver is a citizen of Orange County, Florida. Mrs. Cliver received healthcare services through Florida Complete Care in June of 2022. Florida Complete Care utilized the administrative services of ILS. She received notice that her PII was improperly exposed to unauthorized third parties by ILS.

24. The Supplemental Notice of Data Event dated March 14, 2023, stated that Plaintiffs' PII was accessed in the Data Breach, stating:

What Happened?

On July 5, 2022, we experienced an incident involving the inaccessibility of certain computer systems on our network. We responded to the incident immediately and began an investigation with the assistance of outside cybersecurity specialists. Through our response efforts, we learned that an unauthorized actor obtained access to certain ILS systems between June 30 and July 5, 2022. During that period, some information stored on the ILS network was acquired by the unauthorized actor, and other information was accessible and potentially viewed. Upon containing the incident and reconnecting our computer systems, we conducted a comprehensive review to understand the scope of potentially affected information and identify the individuals to whom such information relates. We received the results of this review on January 17, 2023, and then worked as quickly as possible to validate the results and provide notice to potentially impacted individuals and affiliated data owners, as required under applicable law and contract.

What Information was Affected?

The types of impacted information varies by individual and could have included: name, address, date of birth, driver's license, state identification, Social Security number, financial account information, medical record number, Medicare or Medicaid identification, CIN#, mental or physical treatment/condition information, food delivery information, diagnosis code or diagnosis information, admission/discharge date, prescription information, billing/claims information, patient name, and health insurance information.

Defendant Independent Living Systems, LLC

25. Defendant is a Florida limited liability company with its principal place of business in Miami, Florida. According to Defendant's filings with the Florida Department of State, all members of Defendant (as a limited liability company) are residents and citizens of Florida and have an apparent intention to remain domiciled in Florida.

26. Defendant holds itself out as an industry leader in home and community-based healthcare administrative services to "high-cost complex member populations in the Medicare, Medicaid, and Dual-Eligible Market."[4] To conduct its business, Defendant requires the collection

[4] https://ilshealth.com/ (last visited March 20, 2023).

of PII.

JURISDICTION & VENUE

27. This Court has subject matter jurisdiction over this action under 28 U.S.C. §1332(d) because this is a class action wherein the amount in controversy exceeds $5,000,000, exclusive of interest and costs, there are more than 100 members of the proposed class, and at least one Class Member is a citizen of a different state from Defendant to establish minimal diversity.

28. Defendant is a citizen of Florida because it is a limited liability company formed under Florida law with its principal place of business located in this district at 4601 NW 7th Ave, Miami, FL 33127. The Company operates its business in and outside of Florida.

29. The Southern District of Florida has personal jurisdiction over Defendant because it conducts substantial business in Florida and this district and collected and/or stored the PII of Plaintiffs and Class Members in this district.

30. Venue is proper in this district under 28 U.S.C. §§1391(b) because Defendant operates in this district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

FACTUAL ALLEGATIONS

Defendant Acquires, Collects, and Maintains Plaintiffs' and Class Members' PII

31. Defendant provides administrative and other services in connection with healthcare for the seriously ill, a vulnerable population. During the process of providing its services, Defendant required Plaintiffs and Class Members to provide their highly sensitive PII to Defendant.

28. Defendant, in its Privacy Policy, promises to protect Plaintiffs' and Class Members'

PII.[5] Despite the representations in the Privacy Policy, Defendant failed to protect Plaintiffs' and Class Members' PII because an unauthorized actor accessed Plaintiffs' and Class Members' PII during the Data Breach without their consent.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class Members' PII, Defendant assumed legal and equitable duties to those individuals and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure. Said differently, by collecting this information, Defendant has an obligation to protect PII.

30. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Defendant was required to keep Plaintiffs' and Class Members' PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

31. An unauthorized actor gained access to ILS's computer systems between June 30 and July 5, 2022. During that period, PII that was stored on Defendant's computer systems was accessed and viewed by the unauthorized actor. Defendant later determined that the PII accessed and viewed included Class Members' PII. The Data Breach was so serious that it rendered portions of ILS's computer systems inoperable. The Company did not receive the results of the review of the circumstances underlying the Data Breach until seven (7) months later in January of 2023. Thereafter, ILS "validated" the results and issued notice to impacted individuals in March of 2023.

[5] Defendant's Privacy Policy, https://ilshealth.com/privacy-policy/ (last visited Mar. 21, 2023) ("We are required by law to maintain the privacy and security of your protected health information. We implement a variety of security measures to maintain the safety of your personal information when you access your personal information.").

This was a follow-up to the earlier preliminary notice posted by the Company on its website.

32. As required by state laws across the country, Defendant sent templates of the Notice of Data Breach Letter to state attorneys general. Specifically, Defendant sent a template of the Notice of Data Breach Letter to the Maine Attorney General and identified that approximately 4,226,508 individuals like Plaintiffs had their PII accessed, exfiltrated, and/or compromised on the Data Breach.[6]

33. The Data Breach occurred because Defendant did not implement adequate and reasonable cyber-security procedures and protocols to protect the PII of Plaintiffs and Class Members. Because Defendant's data security protocols and practices were deficient, unauthorized person(s) were able to access, view, and/or exfiltrate Plaintiffs' and Class Members' PII. Notably, in its March 14, 2023 Supplemental Notice of Data Event, the Company acknowledged that "it promptly took steps to mitigate any risk of compromise to information and to better prevent a similar event from reoccurring."[7] These actions included: "(1) fortifying the security of our firewall; (2) utilizing the forensic specialists engaged to monitor our network and remediate any suspicious activity identified; (3) rotating and increasing the complexity of all users' credentials, and (4) providing notification to potentially affected individuals as quickly as possible." Defendant also claims to have "enhanc[ed] our existing training protocols and other internal procedures that relate to data protection and security."

34. The fact that Defendant enhanced its security features post-Data Breach indicates Defendant's cybersecurity measures were inadequate, negligent, and lacking at the time of the Data Breach.

---

6 https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec.shtml (last visited Mar. 21, 2023).

7 https://ilshealth.com/supplemental-data-notice (last visited Mar. 21, 2023).

35. In its March 14, 2023 Supplemental Notice of Data Event, Defendant disclosed that the types of information impacted by the Data Breach include individuals': "name, address, date of birth, driver's license, state identification, Social Security number, financial account information, medical record number, Medicare or Medicaid identification, CIN#, mental or physical treatment/condition information, food delivery information, diagnosis code or diagnosis information, admission/discharge date, prescription information, billing/claims information, patient name, and health insurance information."

36. Upon information and belief, the data accessed in the Data Breach was then exfiltrated and sold or publicly posted on the internet.

37. The Notice of Data Event Letter sent to Class Members offered them a limited time membership to credit monitoring services. This is wholly inadequate because data breach victims and other unauthorized disclosures commonly face multiple years of ongoing identity theft. Indeed, Defendant informed Class Members to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, …."[8]

38. The Notice of Data Event Letter sent to Class Members also suggested several additional time-consuming steps that Plaintiffs and Class Members could take to protect themselves as a result of Data Breach, such as fraud alerts, credit freezes, and/or contacting government authorities.

39. Based on Defendant's urging Plaintiffs and Class Members to take these mitigating actions, as well as its decision to provide victims with credit monitoring services, it is abundantly clear that the perils from the Data Breach are real and concrete.

---

[8] *See, e.g.*, template of the Notice of Data Event Letter submitted to the Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec.shtml (last visited Mar. 21, 2023).

40. Despite the publicly available knowledge of the continued compromises of PII, Defendant's approach to maintaining the privacy of Plaintiffs' and Class Members' PII was inadequate, unreasonable, negligent, and reckless. This is evidenced by Defendants' acknowledgement that additional steps are being taken to further enhance its existing security measures. Defendant's statement admits that at the time of the Data Breach, Defendant's technical and cybersecurity capabilities were inadequate, which in turn, caused the Data Breach and the divulgence of Plaintiffs' and Class Members' PII.

41. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- An awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanning of all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Firewalls configured to block access to known malicious IP addresses.
- Patching of operating systems, software, and firmware on devices, including considering use of a centralized patch management system.
- Anti-virus and anti-malware programs set to conduct regular scans automatically.
- Management over the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Access control configurations—including file, directory, and network share permissions—with the principle of the least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email, including considering using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Disabling Remote Desktop protocol (RDP) if it is not being used.

- Application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Executing operating system environments or specific programs in a virtualized environment.

- Categorization of data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

42. To prevent and detect cyber-attacks Defendant could and should have followed the recommendations of the United States Cybersecurity & Infrastructure Security Agency, which called for the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to

verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic…. [9]

43. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

[9] *See* Cybersecurity Advisory, Ransomware Activity Targeting the Healthcare and Public Sector, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a (last accessed March 21, 2023).

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].

44. Given that Defendant was storing the PII of Plaintiffs and Class Members, Defendant could and should have implemented all the above measures to prevent and detect ransomware attacks. *See* also *Cybersecurity Advisory, Ransomware Activity Targeting the Healthcare and Public Sector*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a (last accessed March 21, 2023).

45. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks. The failure to implement some or all the above measures resulted in the data breach and the exposure of over 4.2 million Class Members' PII. Moreover, based on Defendant's notification to the Maine Attorney General, Defendant failed to encrypt the PII on its network and systems, which was negligent in and of itself.

Defendant Knew or Should Have Known of the Risk Because the Healthcare Sector Is Particularly Susceptible to Cyber Attacks

46. Defendant was specifically on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were

targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

47. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year. In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase. That trend continues. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.

48. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable

information stored in their data centers."

49. As a healthcare services provider, ILS knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Class Members as a result of a breach. ILS failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

50. In addition, at a Federal Trade Commission ("FTC") public workshop in 2001 (more than 20 years ago), then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[10]

51. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11]

52. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12] In other words, the FTC's definition of

---

[10] Transcript, *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[11] 17 C.F.R. §248.201 (2013).

[12] *Id*.

"identifying information" includes the precise information lost in this Data Breach by Defendant.

53. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

Social Security Numbers Are Particularly Valuable

54. Defendant's Notice of Data Breach Letter admits that Plaintiffs' and Class Members' Social Security numbers were included in the Data Breach.

55. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[15]

---

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited March 21, 2023).

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited March 21, 2023).

[15] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 20, 2023).

56. It is incredibly difficult to change a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

57. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, name, and date of birth.

58. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

59. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

61. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

62. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s) and thus the significant number of individuals who would be harmed by the exposure of unencrypted data.

63. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[17] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[18]

64. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[19] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed[,] 69 percent reported feelings of fear

---

[17] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.justice.gov/usao-wdmi/file/764151/download.

[18] *See id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. §603.2(a). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 16 C.F.R. §603.2(b)

[19] Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, NortonLifeLock (Mar. 13, 2018), https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html.

related to personal financial safety[,] 60 percent reported anxiety[,] 42 percent reported fearing for the financial security of family members[, and] 8 percent reported feeling suicidal."[20]

65. More recently, the FTC released an updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

66. The FTC has brought enforcement actions against businesses for failing to protect consumers' PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. §45.

67. The United States government and privacy experts acknowledge that it may take much time for identity theft to come to light and be detected because identity thieves may wait years before using the stolen data.

68. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality (*i.e.*, name, address, lean number, and Social Security number), the harms to Plaintiffs and the Class will continue and increase, and Plaintiffs and the Class will continue to be at substantial risk for further imminent and future harm.

69. Plaintiffs and Class Members have suffered real and tangible losses, including but not limited to, the loss in the inherent value of their PII, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case.

70. Despite Defendant's failure to protect Plaintiffs' and Class Members' PII and the

[20] *Id.* (citing *Identity Theft: The Aftermath 2016*™, Identity Theft Resource Center (2016) https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf).

resulting harm Defendant has only offered to provide Plaintiffs and Class Members with one year of credit monitoring.

71. As a result of the Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII are used;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. The continued risk to their PII that is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in Defendant's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

72. In addition to a remedy for the economic harm, Plaintiffs and the Class maintain an undeniable and continuing interest in ensuring that their PII that remains in the possession of Defendant is secure, remains secure, and is not subject to further theft.

Plaintiff Michael Cliver's Experience

73. Plaintiff Michael Cliver was required to provide and did provide his PII in connection with obtaining healthcare and related services provided by Defendant. The PII included, but was not limited to, his name, address, Social Security number, financial account

number, medical, and Medicare information. The Supplemental Notice of Data Event admits that Class Members' PII was accessed in the Data Breach.

74. Plaintiff typically takes measures to protect his PII and is very careful about sharing his PII.

75. Plaintiff stores any documents containing his PII in a safe and secure location. He diligently chooses unique usernames and passwords for his online accounts.

76. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach.

77. As a result of the Data Breach, Plaintiff must monitor his accounts and credit scores and has sustained emotional distress. Plaintiff will need to spend additional time and effort opening new accounts. Because of the Data Breach, Plaintiff will have time taken from other obligations.

78. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

79. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

80. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security and Medicare numbers, being placed in the hands of criminals.

81. As a result of the Data Breach, Plaintiff is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come. To date, Defendant failed to either adequately protect Plaintiffs and Class Members or to compensate them for their injuries sustained in this Data Breach. The offer of identity monitoring services for a limited

number of months is wholly insufficient to cover the current and future harm.

Plaintiff Mary Cliver's Experience

82. Plaintiff Mary Cliver was required to provide and did provide her PII in connection with obtaining healthcare services provided by Defendant. The PII included, but was not limited to, her name, address, Social Security number, financial account number, and medical information. The Supplemental Notice of Data Event admits that Class Members' PII was accessed in the Data Breach.

83. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII.

84. Plaintiff stores any documents containing her PII in a safe and secure location. She diligently chooses unique usernames and passwords for her online accounts.

85. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach.

86. As a result of the Data Breach, Plaintiff must monitor her accounts and credit scores and has sustained emotional distress. Plaintiff will need to spend additional time and effort opening new accounts. Because of the Data Breach, Plaintiff will have time taken from other obligations.

87. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

88. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

89. Plaintiff has suffered imminent and impending injury arising from the substantially

increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of criminals.

90. As a result of the Data Breach, Plaintiff is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

91. To date, Defendant failed to either adequately protect Plaintiffs and Class Members or to compensate them for their injuries sustained in this Data Breach.

Defendant Violated the FTC Act

92. Section 5 of the FTC Act, 15 U.S.C. §45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

93. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

CLASS ACTION ALLEGATIONS

94. Pursuant to the provisions of Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs seeks to bring this class action on behalf of herself and a nationwide class (the "Nationwide Class") defined as follows:

> **All persons whose PII was accessed and/or acquired in the data incident that is the subject of the March 2023 Notice of Data Incident.**

95. Excluded from the Class are Defendant; officers, directors, and employees of

Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

96. Plaintiffs reserves the right to modify and/or amend the Nationwide Class, including, but not limited to, creating additional subclasses, as necessary.

97. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

98. All Class Members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

99. ***Numerosity***. Consistent with Fed. R. Civ. P. 23(a)(1), the Nationwide Class is so numerous that joinder of all members is impracticable. While the exact number of Nationwide Class Members is unknown, upon information and belief, it is in excess of 4.2 million and it is almost certain that it contains at least 100 individuals.

100. ***Commonality and Predominance***. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class Members. Such common questions include:

a. whether Defendant engaged in the wrongful conduct alleged in this Complaint;

b. whether Defendant's conduct was unfair, unconscionable, and/or unlawful;

c. whether Defendant failed to implement and maintain adequate and reasonable systems and security procedures and practices to protect Plaintiffs' and Class Members' PII;

d. whether Defendant owed a duty to Plaintiffs and Class Members to adequately protect their PII and to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

e. whether Defendant breached its duties to protect the PII of Plaintiffs and Class Members by failing to provide adequate data security and failing to provide appropriate and adequate notice of the Data Breach to Plaintiffs and Class Members;

f. whether Defendant's conduct was negligent;

g. whether Defendant knew or should have known that its computer systems were vulnerable to being compromised;

h. whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Plaintiffs' and Class Members' PII;

i. whether Defendant wrongfully or unlawfully failed to inform Plaintiffs and Class Members that it did not maintain data security practices adequate to reasonably safeguard Plaintiffs' and Class Members' PII;

j. whether Plaintiffs and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);

k. whether Plaintiffs and Class Members are entitled to recover damages; and

l. whether Plaintiffs and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

101. ***Typicality***. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of the claims of other Class Members in that Plaintiffs, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiffs and all Class Members were injured through the misconduct of Defendant and assert the same claims for relief.

102. ***Adequacy***. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs are members of the Class they seek to represent; are committed to pursuing this matter against Defendant to obtain relief for the Class; and have no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiffs retained counsel who are competent and experienced in litigating class

actions and complex litigation, including privacy litigation of this kind. Plaintiffs and their counsel intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

103. ***Superiority***. Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiffs knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

104. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3) because the common questions of law or fact predominate over any questions affecting individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

105. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief

may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

106. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retain possession of Plaintiffs' and Class Members' PII, and has not been forced to change its practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

107. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Plaintiffs' and Class Members' PII was accessed, compromised, or stolen in the Data Breach;

b. whether Defendant owed a legal duty to Plaintiffs and the Class Members;

c. whether Defendant failed to take adequate and reasonable steps to safeguard the PII of Plaintiffs and Class Members;

d. whether Defendant failed to adequately monitor its data security systems;

e. whether Defendant failed to comply with applicable laws, regulations, and industry standards relating to data security;

f. whether Defendant knew or should have known that it did not employ adequate and reasonable measures to keep Plaintiffs' and Class members' PII secure; and

g. whether Defendant's adherence to FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

108. Plaintiffs repeat and re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 107.

109. Plaintiffs brings this claim on behalf of themselves and the Nationwide Class.

110. Defendant required Plaintiffs and Class Members to submit sensitive personal information, including their PII, to obtain healthcare services. Defendant collected, stored, used, and benefited from the non-public PII of Plaintiffs and Class Members in the provision of providing healthcare to Plaintiffs and Class Members.

111. Plaintiffs and Class Members entrusted Defendant with their PII and Defendant was fully cognizant of the value and importance of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

112. Defendant negligently created a dangerous situation by failing to take adequate and reasonable steps to safeguard Plaintiffs' and Class Members' sensitive PII from unauthorized release or theft.

113. Defendant owed an independent duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII, and preventing the PII from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

114. Defendant was required to prevent foreseeable harm to Plaintiffs and Class

Members. Accordingly, Defendant had a duty to take adequate and reasonable steps to safeguard their sensitive PII from unauthorized release or theft. Defendant's duties, included, but were not limited to: (1) designing, maintaining, and testing its data security systems, data storage architecture, and data security protocols to ensure Plaintiffs' and Class Members' PII in its possession was adequately secured and protected; (2) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding its security vulnerabilities and potential compromise of the PII of Plaintiffs and Class Members; and (4) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

115. Defendant owed a common law duty to prevent foreseeable harm to Plaintiffs and Class Members. The duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices of Defendant in its collection, storage, and use of PII from Plaintiffs and Class Members. It was foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PII because malicious actors routinely attempt to steal such information for use in nefarious purposes.

116. Defendant's obligation to use adequate and reasonable security measures also arose because Defendant collected, stored, and used the PII of Plaintiffs and Class Members for the procurement and provision of healthcare services.

117. Additionally, the policy of preventing future harm weighs in favor of finding a Defendant had a duty towards Plaintiffs and Class Members.

118. Defendant also owed a duty to timely disclose the material fact that its computer systems and data security practices and protocols were inadequate to safeguard users' personal,

health, and financial data from theft.

119. The injuries suffered by Plaintiffs and Class Members were proximately and directly caused by Defendant's failure to follow reasonable, industry standard security measures to protect Plaintiffs' and Class Members' PII.

120. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take additional steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

121. If Defendant had implemented the requisite, industry-standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the PII of Plaintiffs and Class Members.

122. Defendant breached these duties through the conduct alleged here in this Complaint by, including without limitation, failing to protect the PII in its possession; failing to maintain adequate computer systems and allowing unauthorized access to and exfiltration of Plaintiffs' and Class Members' PII; failing to disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard the PII in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiffs and Class Members the material fact of the Data Breach.

123. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised. And, as a direct and proximate result of Defendant's failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the PII of Plaintiffs and Class Members was accessed by ill-intentioned individuals who could and will use the information to commit identity or

financial fraud. Plaintiffs and Class Members face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

124. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII of collected from Class Members and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and Class Members.

125. It was foreseeable that Defendant's failure to exercise reasonable care to safeguard the PII in its possession or control would lead to one or more types of injury to Plaintiffs and Class Members. The Data Breach was also foreseeable given the known, high frequency of cyberattacks and data breaches in the healthcare industry.

126. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing PII, the critical importance of providing adequate security of PII, the current cyber scams being perpetrated on PII, and that it had inadequate protocols, including security protocols in place to secure the PII of Plaintiffs and Class Members.

127. Defendant's own conduct created the foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included its failure to take the steps and opportunities to prevent the Data Breach and its failure to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiffs and Class Members.

128. Plaintiffs and Class Members have no ability to protect their PII that was and is in Defendant's possession. Defendant alone was, and is in, a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

129. As a direct and proximate result of Defendant's negligence as alleged above, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII are used;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. The continued risk to their PII that is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in Defendant's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

130. Pursuant to the FTC Act, 15 U.S.C. §45, Defendant had a duty to provide fair and adequate computer systems and data security measures to safeguard the PII of Plaintiffs and Class Members.

131. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The

FTC publications and orders described above also form part of the basis of Defendant's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

132. Defendant solicited, gathered, and stored PII of Plaintiffs and Class Members to facilitate transactions that affect commerce.

133. Defendant's violation of the FTC Act (and similar state statutes) constitutes negligence.

134. Plaintiffs and Class Members are within the class of persons that the FTC Act (and similar state statutes) were intended to protect.

135. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act (and similar state statutes), seeks to prevent. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ adequate and reasonable data security measures, caused the same harm as that suffered by Plaintiffs and Class Members.

136. As a direct and proximate result of Defendant's violations of the above-mentioned statutes (and similar state statutes), Plaintiffs and Class Members have suffered, and continue to suffer, damages arising from the Data Breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

RELIEF REQUESTED

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, respectfully requests the following relief:

a. An order certifying this case as a class action on behalf of the Class, defined above, appointing Plaintiffs as Class representative and appointing the undersigned counsel as Class counsel;

b. A mandatory injunction directing Defendant to adequately safeguard Plaintiffs'

and the Class's PII by implementing improved security procedures and measures as outlined above;

c. An award of other declaratory, injunctive, and equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

d. An award of restitution and compensatory, consequential, and general damages to Plaintiffs and Class Members, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;

e. An award of actual or statutory damages to Plaintiffs and Class Members in an amount to be determined at trial or by this Court;

f. An award of reasonable litigation expenses and costs and attorneys' fees to the extent allowed by law;

g. An award to Plaintiffs and Class Members of pre- and post-judgment interest, to the extent allowable; and

h. Award of such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demands a trial by jury of any and all issues in this action so triable as of right.

DATED: March 22, 2023

GEORGE FELDMAN MCDONALD, PLLC

/s/ David J. George

David J. George (FBN 898570)
Brittany L. Brown (FBN 105071)
9897 Lake Worth Drive, Suite 302
Lake Worth, Florida 33467
Telephone: (561) 232-6002
Fax: (888) 421-4173
dgeorge@4-Justice.com
bbrown@ 4-Justice.com
eservice@4-Justice.com

GEORGE FELDMAN MCDONALD, PLLC

Lori G. Feldman (*pro hac vice* forthcoming)
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
Fax: (888) 421-4173
lfeldman@ 4-Justice.com

EMERSON FIRM, PLLC

John G. Emerson (*pro hac vice* forthcoming)
2500 Wilcrest Drive
Suite 300
Houston, TX 77042-2754
Telephone: (800) 551-8649
Fax: (501) 2864659
jemerson@emersonfirm.com

Counsel for Plaintiffs and the Putative Class